BT Means Business

Secure your future of work

How to protect your people, workplaces and business

Introduction

The future of work should be based on strong foundations. One that will support innovation and growth, and create a better, more secure collaboration environment with technology partners who help build digital transformation strategies.

But accelerated digital transformation has changed the threat landscape and provided the opportunity for cyber attacks to increase.

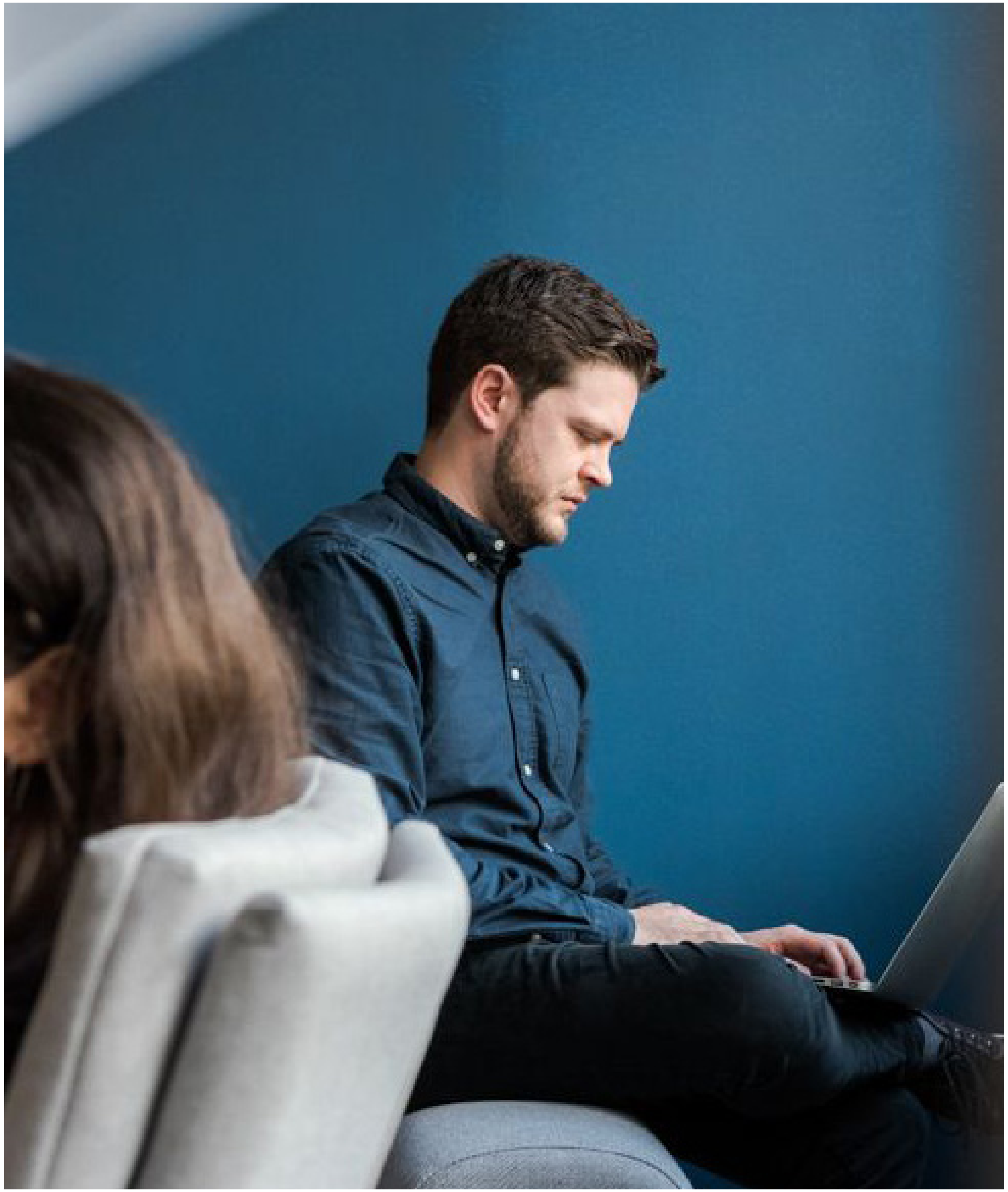
In the UK, 72 percent of large enterprises identified cyber breaches in 2021, according to the **Department of Digital Culture, Media & Sport.** Within the group of organisations reporting cyber attacks, 31 percent of businesses estimate they were attacked at least once a week. The most common threat was phishing attempts – staff receiving fraudulent emails or being directed to fraudulent websites. But more vigilant businesses identified more sophisticated attacks as well, like denial-of-service attacks, the takeover of an organisation or users' account, or ransomware.

More fluid working models and the move to cloud and Edge mean that these instances are predicted to **rise in the next year.**

The C-Suite recognises this new imperative. Research by the **Independent Directors Council** found that 67 percent of CISOs prioritised cybersecurity above all other business considerations. More interestingly, 76 percent of respondents believed that managing cyber risk is so important that companies will start appointing CISOs as CEOs.

However, many are unsure of how to deploy the right tools so that malicious attacks **are successfully detected** and **cloud security risks** are accurately measured to prevent the loss of intellectual property, competitive insights, or consumer trust.

But security does not need to be complicated. Ultimately, all organisations want to protect their people, workplaces and overall business. And with the right expertise, knowing where to start is easy. By taking the appropriate steps, every employer can help shield their institutions against reputational and financial risk. What's more, they'll give their teams access to the best tools and devices to improve and secure the end-user experience as the future of work continues to evolve.



Five areas you must secure to protect your entire estate

Protect

1. Secure your network

In recent years, organisations have migrated assets, data, and applications online and, especially since 2020, opened up their private networks to remote access to enable their teams to work from anywhere.

While this accelerated their digital transformation a lot faster than planned, it created multiple points of ingress and egress, which means many security teams didn't have enough time to prepare for the new risks they had to take on.

Companies are now tasked with opening up their networks, without exposing their data and operations. Networks can be physical, virtual, MPLS-based, or something else – but all need to be protected adequately to minimise the impact of threats.

Some have chosen SD-WAN to connect disparate operations across a wide range of locations and prioritise traffic, as SD-WAN is more dynamic and flexible than solely using MPLS. Implementing SD-WAN correctly could enhance every business' security strategy. But it still needs securing. A range of controls are available depending on your individual requirements, including Managed Firewall and Managed Cloud Security.

2. Secure your cloud

By 2023, 70 percent of enterprise workloads will be **deployed in cloud infrastructure** and platform services, up from 40 percent in 2020.

While cloud adoption is picking up the pace, businesses often undermine associated risks or lack the knowledge on how to safely integrate it into their existing architecture. Many assume the likes of Amazon Web Services take sole responsibility for security in the cloud, **when that isn't the case.** Two thirds of UK business leaders expect a jump in attacks on their cloud services over the next year, but only **41 percent profess to understand the risks.** Threats include data loss, lack of visibility and security breaches.

To ensure cloud services are only accessed by the right people, businesses must gain full visibility and control over their services.

Solutions like **Cloud Access Security Broker (CASB)** that sits between a cloud provider's and an on-premises cloud infrastructure can help businesses manage security across all their applications. It helps provide protection from things like shadow IT and critical data loss.

Backing up data is another key consideration, as is securing your internet connection to cloud applications with a web proxy or virtual firewall. This will ensure that information stored on external cloud computing platforms remain safe.

3. Secure your devices

In a hybrid work environment, users and devices are no longer inside a fixed corporate perimeter. That means IT departments are left to deal with different management systems and configurations to accommodate different platforms and data locations.

Exacerbating this complexity, the average person **now uses 3.5 collaboration tools** and a third of us use six.

However, blurred boundaries of devices, data and content have caused new vulnerabilities. Endpoint attacks are responsible for up to 50 percent of all enterprise data breaches and **69 percent of organisations** suffered a cybersecurity incident as a direct result of teams working remotely. Additionally, since COVID, employees are **85 percent more likely to leak files.**

To put users at the heart of the organisation and drive secure collaboration when employees are mobile, business leaders must choose a cloud-based endpoint protection solution that protects all users, no matter where they're working from. Deploying Next-Generation Antivirus (NGAV) that combines artificial intelligence, behavioural detection, machine learning algorithms, and exploit mitigation, will help anticipate and immediately prevent known and unknown threats.

Most importantly, businesses must have a consistent security policy – by regularly updating and patching servers, computers, security cameras, and other devices. And by ensuring that security policies and solutions protect all devices, whether company-issued or BYOD (bring your own device). One solution would be to take out an MDM (mobile device management) solution, to manage all devices centrally.

4. Secure your supply chain

Online retail sales growth for 2020 was up **36 percent year-on-year** – the highest annual growth seen since 2007. Organisations struggled to hasten production timelines and meet voracious demands.

And other factors, such as the lack of delivery drivers and increased freight costs, pushed businesses to find new ways to maintain productivity while increasing efficiency and reducing overheads.

The scramble to meet these ambitious production targets meant many businesses adopted technology haphazardly, leaving gaps in their cybersecurity. Supply chain attacks, designed to exploit trusted relationships between organisations and their external parties (like partnerships, vendor relationships, or the use of third-party software) **surged during this time.**

The most notable example was the SolarWinds attack that saw the company's widely used software compromised at the source, putting as many as 18,000 SolarWinds customers at risk. They attack gave hackers access into 100 networks – including those of Fortune 500 companies like Microsoft and the US Justice Department, State Department, and NASA.

Businesses can help secure their supply chains by: minimising supplier access to networks and workplaces, categorising suppliers with different levels of access based on risk scores, continuously reviewing supplier access, and having contingency plans in place for breaches. Crucially, businesses should establish that suppliers they work with are secure themselves and don't pose a risk to your company.

5. Secure your human firewall

Working from home is a change in mindset and behaviour – one that cybercriminals exploited during the pandemic. The decreased protection that came with dispersed teams and a greater reliance on technology, meant businesses throughout the country saw a rise in phishing and malware attacks.

Many hacking campaigns were spread through emails and social media. These targeted employees directly, tapping into their sense of urgency, worry and fear.

That's why businesses must take the human factor of their security strategy into account, looking at how their teams are using newly adopted tools and technologies. Helping employees understand the policies and procedures around data security – and raising awareness about cyber attacks – can help staff behave safely online. Businesses should also invest in regular training to ensure employees can spot threats, such as phishing attacks.

Businesses need security expertise

The accelerated pace of change of the last two years has caused big advances in some areas, slow progress in others.

Only 41 percent of organisations report that their IT security team is effective in determining and closing gaps in IT security infrastructure and 53 percent of leaders don’t know if their cybersecurity tools are working.

Businesses need security expertise. Especially from consultants with deep insight and experience to pinpoint significant threats, ensure compliance and establish control. With the right partner, they can draw a roadmap to move away from legacy infrastructure and scale for the future – all while improving staff interaction, collaboration and embracing innovation.

The right partner

Partner

The cyber threat landscape is evolving and as customers embrace new ways of working, the need to invest in secure foundations has never been greater.

And with a **cyberskills shortage**, now is the time to focus on the bigger picture: preparing people, workplaces and the overall business for a working culture that thrives on innovation and ideas. BT can help you achieve this.

BT is recognised for its ability to seamlessly integrate its security portfolio with wider network and cloud solutions. We were named **a leader in the IDC MarketScape: Managed Security Services 2022 Vendor Assessment report**, which provides an overview of the competitive fitness of MSSPs in the European market.

BT's security team provides solutions to consumers, governments and businesses around the world, and protects the company's global network against around 200,000 cyber attacks per month.

Our Security division achieved **accreditation from CREST,** one of the cyber industry's most highly regarded industry bodies, in recognition of its leading threat intelligence insight and capabilities.

Our vast reach means we have security operation centres around the globe, providing round-the-clock coverage, and manage 10 million alarms, 15,000 security alerts and 93,000 security devices every year. We also partner with best-in-class security vendors and will collaborate with you to find the best solution for your needs.

BT's experience, knowledge and scale make us uniquely placed to be the future of work partner for British enterprise. With 3000+ dedicated security experts, we've been protecting ourselves, our customers – small, medium & large businesses – and the UK's critical national infrastructure for over 70 years.

The future of work isn't a tomorrow thing, it's today. We can deliver the end-to-end digital transformation that puts businesses on a sure path to greater productivity, effectiveness and growth.

To find out more contact your account manager or call 0800 7076313

Offices Worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

July 2022